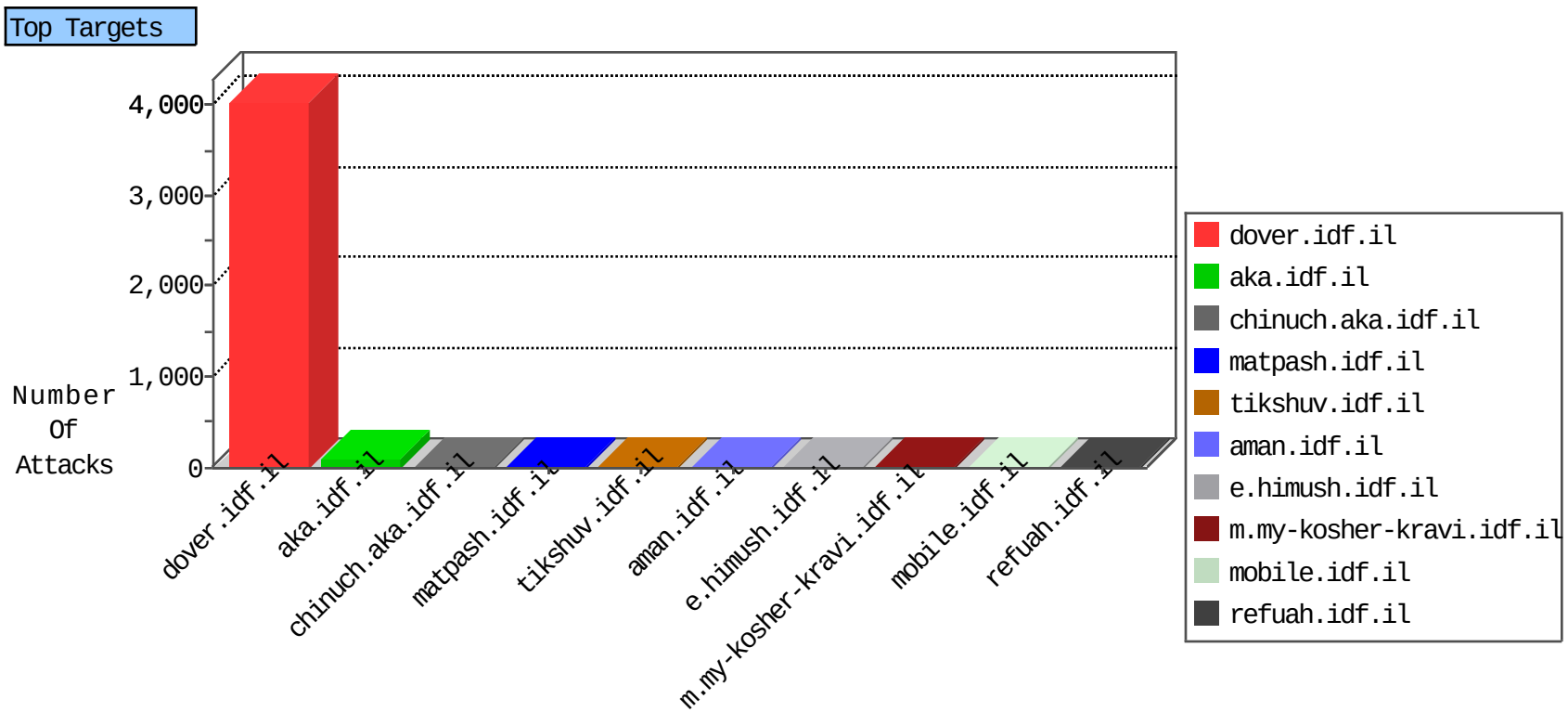
04-27-2016-05:04:02 to 04-27-2016-06:04:02

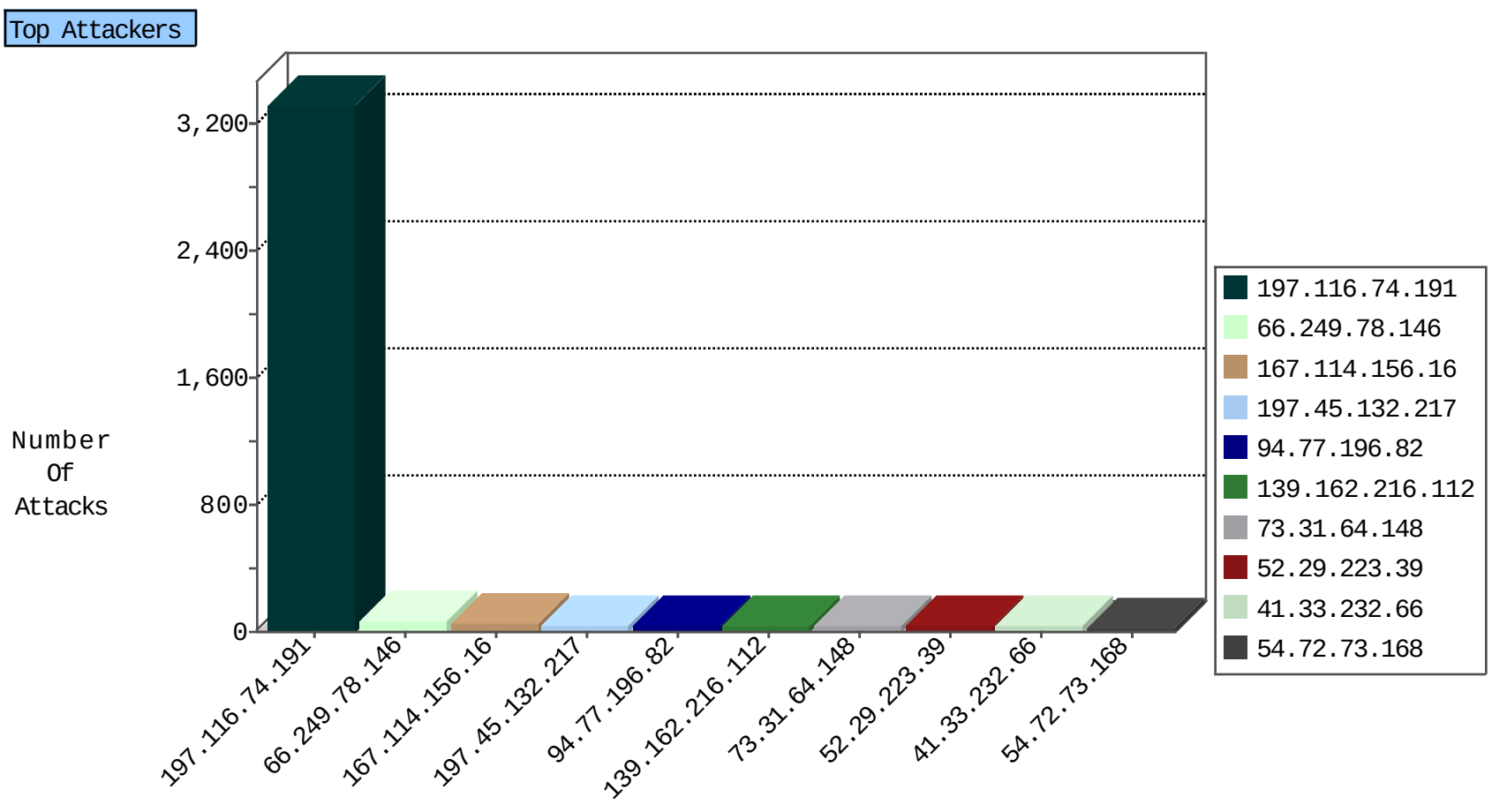
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

04-27-2016-05:04:02 to 04-27-2016-06:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	3630
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	823
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	125
197.116.74.191	Algeria	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	55
120.132.50.135	China	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	4
123.59.59.52	China	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	4
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
185.94.111.1	Russian Federation	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1

04-27-2016-05:04:02 to 04-27-2016-06:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.107.57	France	147.237.0.34	tikshuv.idf.il	10711: HTTP: ZmEu Vulnerability Scanner	Block	1
62.210.107.57	France	147.237.0.15	kosher-kravi.idf.il	10711: HTTP: ZmEu Vulnerability Scanner	Block	1
62.210.107.57	France	147.237.0.17	m.my-kosher-kravi.idf.il	10711: HTTP: ZmEu Vulnerability Scanner	Block	1

04-27-2016-05:04:02 to 04-27-2016-06:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
174.37.194.144	147.237.77.176	United States	matpash.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
124.105.93.73	147.237.0.34	Philippines	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
122.52.169.104	147.237.76.34	Philippines	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.171.122.176	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -f -sS	1
76.181.249.213	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
13.92.84.22	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 3072	1
197.116.74.191	147.237.77.216	Algeria	dover.idf.il	portscan: TCP Distributed Portscan	1
13.92.84.22	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -f -sS	1
195.216.176.244	147.237.72.156	Latvia	aman.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
190.253.212.51	147.237.76.44	Colombia	e.refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
174.37.194.144	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 4096	1
122.160.28.50	147.237.0.16	India	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.171.122.176	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 2048	1
80.82.78.38	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.211	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
13.92.84.22	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 2048	1
195.216.176.244	147.237.72.156	Latvia	aman.idf.il	ET SCAN NMAP -sS window 1024	1

04-27-2016-05:04:02 to 04-27-2016-06:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.116.74.191	Algeria	147.237.77.216	dover.idf.il	drop		drop	1841
197.116.74.191	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	803
197.116.74.191	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	565
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	69
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
73.31.64.148	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
162.255.123.34	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
65.123.142.184	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
197.116.74.191	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	22
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
207.46.13.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
158.69.228.18	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
197.116.74.191	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	16
207.46.13.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
40.77.167.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
197.116.74.191	Algeria	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	12
162.243.71.33	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.243.97.21	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.103.160	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
128.242.249.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
40.77.167.31	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
207.119.114.12	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
76.250.147.128	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.28.160.150	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.9.112.6	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
203.133.169.210	Korea, Republic of	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
12.153.8.130	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.0.113.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
104.46.236.214	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
91.217.164.102	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
178.255.215.87	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.184	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
108.23.167.153	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
172.56.21.166	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.64.61.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
95.186.121.32	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.78.199	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-27-2016-05:04:02 to 04-27-2016-06:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
8.37.232.242	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
66.249.93.111	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
174.37.194.144	United States	147.237.77.176	matpash.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/3044.jpg	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
186.154.25.123	Colombia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/spanish	Block	1
66.249.66.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/2294.jpg	Block	1
120.132.50.135	China	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.elong.com/894-he/chinuch.aspx	Block	1
197.116.74.191	Algeria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
123.59.59.52	China	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.qyer.com/894-he/chinuch.aspx	Block	1
40.77.167.8	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/smalim/faq.aspx	None	1
208.90.57.196	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/www.youtube.com/embed/02xlfsfhjyk	Block	1
66.249.93.119	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.39.27	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluim/horaot/news/news.asp	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
216.218.206.66	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
88.86.99.166	Czech Republic	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in tikshuv.idf.il/site/general.aspx	Block	1

04-27-2016-05:04:02 to 04-27-2016-06:04:02